International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Secure Wireless Body Area Networks for Healthcare Applications

S. Ananthakumaran, R. Bhavani, K. Mohideen Pitchai

Abstract*: Wireless Body Area Network (WBAN) is the most important recent trending approaches to provide Medical care for patients through remote monitoring and data collection using body sensors. It's a well-known system offering a high standard of security and also privacy. Therefore, it provides us a very big interest for discussing the issues of privacy and security in WBAN. In this paper, the architecture of WBAN communication network, various safety threats and it's measures, several types of research methodologies to secure health records and research issues are reviewed on the basis of various secure routing protocols of recent publications. Also, this paper tabulated the detailed comparison study of analysis of security requirements, resistance to various attacks, computing costs during authentication and running time between the application provider and the customer. At last, open fields are investigated for future research.

Keywords: Wireless Body Area Network protocol, Security, Privacy, Threats, Attacks.

I. INTRODUCTION

Based on the data from the perspective of the world population [1]: the Revision of 2017, addresses that the number of elderly people, 60 years of age or older, increased from 962 million in the year of 2017 to 201 billion in the year of 2050 and 3.1 billion in the year of 2100. Since the aged people belonging to this age group are going to take risk with different types of health problems, they may require more frequent medical treatment to live in the world. So, it is inconvenient for them suppose they want to move for long distance from home place to the medical center.

At present, in most of the regions in the world with economically forwarded and back-wording countries, traditional medical care is following and these caring centers are monitoring the patients in particular time of a day or a week. This style of diagnosis process is not yielding fruitful result to reduce their health issue. Therefore, a continuous patient monitoring system is needed to achieve better treatment for this age group of patients.

Recently, wireless body area network (WBAN) is emerging trends to enable Real time and ongoing tracking in different areas, including telemedicine. The WBAN contains small size actuators and sensors. These sensor nodes are positioned either directly on a patient's body or under the skin of the patient, to capture the bio-signals like Electro Cardio Gram (ECG), Elector Encephalon Gram (EEG), pressure and glucose level of Blood, movement of body and heart rate. These sensors are communicating wirelessly among themselves. This type of sensor network allows patients to be released early from medical center and also possible to monitor their conditions at home. Though the patients are discharge from nursing home, their disease related data is available in the hospital server. Here, the database in the hospital should be kept as secret as possible.

Generally in WBAN, patients' health related diagnosis processes are monitoring from the medical center. During this course of action data or observations are mutually exchanged on either side. The patient would send the bio-signals to medical centers and from the medical center practitioners will instruct the patient based on received data of bio-signals. Suppose during mutual communication data may be interrupted, intercepted or impersonated. At this instance on either side of the communication may receive the incorrect instruction or data. So, these attacks sometimes end the patients' life by giving incorrect doses based received wrong observation by the care takers. At this scenario, the communicating parties on either side should ensure their authenticity and also ensure about message authentication before acting upon data. Thus, there is urgent need for user authentication, mutual authentication. These two authentications are very essential for remote monitoring of the patients. In order to keep data in hospital database and to entrust the authentication process, it requires secret key of encryption scheme. Therefore patient-related data security and privacy are two essential concepts. The authors in [4] represented that data security means to ensure its integrity, validity and authenticity and information protection, information can only be accessed by persons authorized to view and use it. Even though WBAN is very small network, security and privacy is essential. This scenario motivates us to get in-depth study about security and privacy of WBAN data communication.

Manuscript published on November 30, 2019.
* Correspondence Author
R.Bhavani*, Assistant Professor, Electrical and Electronics Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India. Email: bavanir@mepcoeng.ac.in.
Dr.S.Ananthakumaran, Associate Professor, Department of Computer Science and Engineering,, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. Email: bhashkumaran@gmail.com.
K.Mohideen Pitchai, Assistant Professor, Department of Computer Science and Engineering National Engineering College, Kovilpatti, Tamilnadu, India.

II. WBAN COMMUNICATION ARCHITECTURE

In the 21st century, rapid growth and advances in the development of microelectronics and micro-electro-mechanical system (MEMS), small and smart devices have been found out. This component is called as sensor. Sensors are playing a vital role in day-to-day life like home automation, precision agriculture, inventory, remote monitoring, intelligent transportation system, sports, entertainment and military.

Distributed sensor nodes are having wireless transceiver and communicate wirelessly to transmit the data, are referred to as a Wireless Sensor Network (WSN).With more than one battery powered sensors can be attached with the patient on/in body or on the clothes to monitor different kind of bio-signals of the person. These signals are categorized like ECG, EEG, blood pressure, glucose level etc. Networking all such kind of sensors is called Wireless Body Area Networks (WBAN).

In terms of realization [3] in nodes are categorized into three types:

- **Implant Node:** This kind of node is either planted under the skin or inside the tissue of the body.
- **Surface Node:** This kind of node is either placed on the surface or 2 cm from the body of the human being.
- **External Node:** This node is not in touch with the human body, but a few centimeters to five meters away from the human body.

A node is a specialized and independent device with communication capability. The devices are spread on/in the body of centralized network architecture with fixed location is application specific. There are three types of nodes are considered in WBAN such as sensors, actuator, and personal device. As for communication architecture as shown in Fig. 1 and as represented in [4], the data communication is separated into three different types.

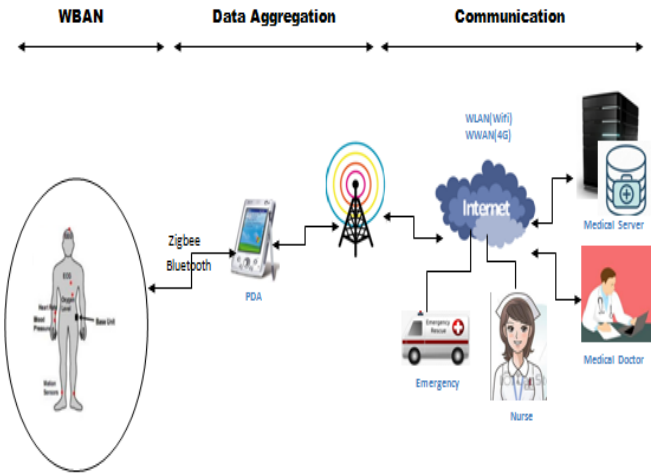

Fig. 1. WBAN Communication Architecture

- **Tier-1**: Intra-BAN Communication - the transmission range of a device here is approximately 2 meters. Various types of sensors are used to observe the bio-signals of human body and forward to coordinator which is located in Tier-1.
- **Tier-2**: Inter-BAN Communication – here data transmission takes place between node coordinator and Access Points (AP). The intention of this zone is to interconnect WBANs with other networks. Moreover this zone is classified into two types based on facilities such as Infrastructure based architecture and Ad-hoc based architecture.
- **Tier-3**: Extra-BAN Communication – this is meant for metropolitan areas and is application specific

III. SECURITY & PRIVACY REQUIREMENTS OF WBAN

WBAN systems are needed some kind of security and privacy in order to keep patients health records as secret as possible. Even though WBAN is resource constrained network, it very important to implement security principles in it. To keep the health records as confidential, as mentioned in [3] the two factors like security and privacy are very essential. The term Security is the protection of data from unconstitutional users when it is being transmitted, collected, processed and also remains safely accumulated. Perfect security architecture of WBAN requires achieving the followings:

- **Efficiency:** Present WBAN is not able to perform cryptographic operation, which consumes more energy. So, fast and lightweight security architecture need to be designed in order to reduce communication overheads and energy consumption.
- **Scalability:** It does not mean only growing the size but also should considered downsizing issues. A node may leave or join the network because the human body is always in movement. In this point of view the security model should be designed.
- **Usability:** Even though the patients using the remote medical treatment via WBAN, they need not be skilled persons to execute the complex professional operation on the devices. So, the architecture is easy and simple for such people.

The reason for what is the need to keep the health records in confidential manner is that, if data is pour out to unauthorized customers, this would lead to multiple of consequences like unable to attend social gathering, losing job, humiliating by others, mental worries and sometimes unable to claim medical insurances. Fig.2 represented in [3], a secure mechanism of the data collection, retrieved only by the authorized person. The important of security and privacy requirements for WBAN architecture is discussed as follows as in [3].

- **Data Confidentiality:** WBAN is an open network is dealing with patients' health record. So, privacy of data is to be maintained from passive and active attacker. Suppose unauthorized access is happened then it could be hazardous to the patients' life. Encryption is a technique can provide best protected data transmission between WBAN node and coordinator node, and moreover it provides confidentiality of data.
- **Data Authentication:** Authentication can be categorized as user authentication and message authentication.

Retrieval Number: D7193118419/2019©BEIESP
DOI:10.35940/ijrte.D7193.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

User authentication means on either side of the communicating parties should ensure that they are the intended party for the further communication. Message authentication means the received message is signed by sender of the message. This can be done by using digital signature.

- **Access Control:** It means that providing access privileges to the concerned stake holders. People may have different capability of knowledge and it is influencing the treatments of the patients. Hence, very clear access control, of medical records, polices has to be defined. It creates goodness to the patient's treatment.
- **Data Integrity:** It measures the accuracy and consistency of the received message. Since WBAN is a open network, an passive attackers can modify and inject unwanted information on the transmitting data. Suppose this modified data is received by received by receiver then it may lead to system failure or cause disaster to the patients. So, in order to avoid this scenario, the received data should be verified for its integrity.

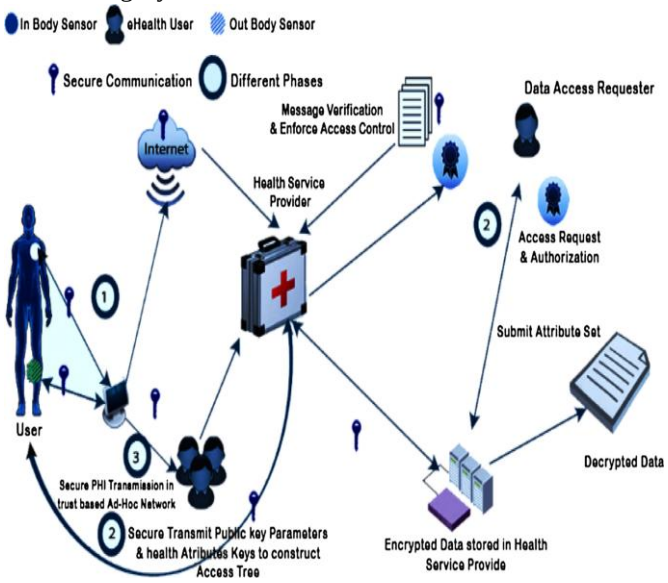

Fig. 2. Security and Privacy in WBAN System

- **Data Availability**: The WBAN data base is containing very important and highly sensitive information. Its service must be available throughout the day for the access of the authenticated patients and medical practitioners. The eve's may attack medical server with Denial of Service (DoS) attack and its leads to unavailability of data accessing. Therefore WBAN architecture must be designed in order to resist the DoS attack.
- **Security Management**: Since the patients are moving from one place to another place, should take care of the body sensors associating and disassociating from one network to another network. In order to transmit data among communicating parties, they should share their secret key. To distribute this secret key encryption and decryption is to be followed [2].
- **Flexibility**: Authorization to access the patients' data should be known on order basis to various care takers who are not essentially listed as being authorized. For an instance, if any one of the patient wants to change the medical center then it is possible to transfer the access control [2].

IV. TESTING SECURITY THREATS & MEASURES

WBAN is an open patients and treatment provider's network. So, there is vulnerable to attack like unauthorized router access, man-in-middle attack, spoofing, DoS attack brute-force attacks [4].

The main objective of the attackers may be availability of the WBAN. Suppose Eve creates unavailability of the resources like health records for some times, this may lead to life-threatening situation. It can be established by DoS attack. Jamming is another attack which blocks a few nodes from transmitting data. This threat leads to packet loss. Security for medical data is very important and must not be avoided. Since medical records are very sensitive, keep them as secure as possible. There are number of security solutions or encryption techniques are proposed till now for WBAN and they are as follows

- **Symmetric Key Encryption:** Initially, WBAN security schemes are set up by symmetrical cryptosystems due to a lack of resources. In the technique, both communicating parties must have the same key that has to be transmitted on other party. So, it has a problem of key distribution and also provides weak security comparatively [2]. Since the sensor's node having limited computation capacity energy, communication rate and memory space, this method is not suited for WBAN..
- **Asymmetric Key Encryption:** Almost most of the literature used a traditional public key cryptosystem (TPKC) [18] for mutual authentication. But it has a complicated modular exponentiation procedure that requires powerful computer equipment or capacity. When deal with WBAN, sensors are having limited abilities. Hence, the computation cost is too high for WBAN.
- **Elliptic Curve Cryptography (ECC):** ECC technique [18] has been used in different scenarios to address the issues of modular exponentiation of TPKC. ECC provides good performance with small key size. When number of users is increasing and the concerned management of certificate is a challengeable task in ECC. Even though ECC is good alternative for TPKC, but not suited for WBAN.
- **Identity based Encryption:** To avoid the management of certificate issues mentioned above, Identity based authentication schemes are proposed. Here, the identity of the user is used as a public key and no authentication certificate is required. But it is designed for Client / Server environment and not suitable for WBAN.
- **Biometric Encryption:** The survey in [2] mentioned that biometric encryption scheme is used for secure communication in biomedical sensor networks.

Here, the key is generated through self-body sensors and distribute the key on other side. Since symmetric key is employed on both sides, this key is used for encrypt and decrypt the data.

V. RESEARCH IN WBAN SECURITY & PRIVACY

For further clarification, few of the needed preliminaries about different authentication schemes are presented in this section.

5.1 Elliptic Curve

Koblitz Koblitz and Miller developed Elliptic Curve Cryptography (ECC). Elliptic curves constitute points on

Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \cup \{\infty\}.$$

A simple Weierstrass elliptic curve equation $E_q(a,b)$ in a field F_q, is defined as a set of {x,y} represented by the formulae $y^2\%q = (x^3+ax+b)\%q$. The values a,b,x,y £F_q and the discriminant $\Delta=4a^3+27b^2 \% q \neq 0$. A 160-bit ECC is equivalent to a 1024-bit RSA key. The ECC's use in safety is based on its relatively small key size and also the complexity of finding solution for Elliptic Curve Discrete Logarithm Problem (ECDLP). ECC is used for authentication for WBAN are [10][13][17][18][21].

5.2 Network Model for Authentication

Most of the literatures related to the Network Model of Mutual Authentication for WBAN are followed as shown in Fig. 3. This network model consists of client, Network Manager and Application Provider. The on-body sensors in WBAN observe the concerned conditions of the human body and transmit physiological data to the controller. Here the authentication is considered between C and AP. Initialization, Registration and Authentication [10][13][17][18][21] are the main algorithmic procedures for each of the authentication protocols.

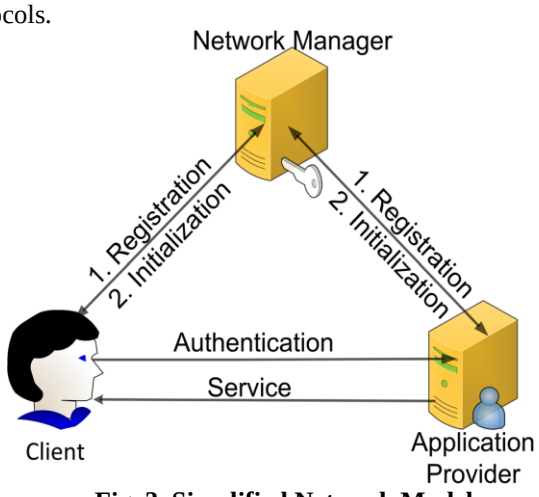

Fig. 3. Simplified Network Model

To authenticate the communicating parties each other, a cryptographic key is obtained from NM after both parties (C and AP) are registered as a communication parties. Assume that NM is as a completely trusted third party and as a Key Generating Center (KGC).

5.3 User or Anonymous Authentication

- **Anonymous Authentication using ECC:** The protocol in [21] is proposed a security model to deal with identity (ID) based anonymous authentication for WBANs using ECC. This model provides customer and application provider authentication, and also provides customer anonymity. Here, the anonymous authentication has been achieved without using bilinear pairing operation and verifier-table for WBAN but with the help of ECC. But the author is unable to provide true client ambiguity because of the pseudo identification of the client is an everlasting value that can be easily traced. The security model is providing enjoyable medical services for the anonymous patient in WBANs. This means that the medical practitioners or nurses need not know about the patient's private information but they need to know about the health-related data only. This scheme uses the network model as shown in Fig. 3 and the performance of the proposed security model has shown better in terms of computational cost and communication cost on client and application provider.
- **Anonymous Authenticated Key Agreement Model:** The client's or patients' personal information is very sensitive and the security for patient's psychological information needs to be ensured. Most of the literature shows that the authentication is using only one key for communication between patient and doctors. But the key need to be updated and therefore it ensures that security of the protocol. The authors in [6] are appended a key updating phase with Initialization, Registration and Authentication phases in the existing security model. Performance analysis of this model has shown that the computational cost in the authentication phase is more efficient than in [24][25]. Suppose the session keys in [24][25] is compromised then these schemes are insecure. In [6], the model is allowing for data communication between client and AP and is updating their session keys to enhance their security. Here authentication phase is more secure than [24][25] by satisfying the properties like forward secrecy, unlinkability, and non-repudiation.
- **Anonymous Authentication using ECC:** The protocol in [18] is proposed a network model as described in Fig. 3 and uses the concepts of ECC and Bilinear Pairing as described in 5.1. This security system works under random oracle model for certificate less authentication scheme.
  The authors assumed that a super singular curve $E(F_p)$ over a finite field $E(F_p)$, G_1 is a repeated addition group stated on $E(F_p)$ with the order of q,E is stated on G_1,where p=512-bit and q=160-bit respectively to compute for both computation cost and communication cost. Let the elements length of G_1 and G2 is 1024-bit and n_T and n_{ID} denote the bit length of the timestamp and the identity respectively.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The communication cost for authentication process between client and authentication provider is more than 4416-bits. Here, the C is a sensor device having limited power while AP has a powerful computing ability. It is [18] an effective authentication system for WBANs to decrease the stress of customer side of WBAN [10]. Thus the performance of the simulation result shows that computation cost of [18] for WBAN has reduced by about 31.58% compared with [22] security model. But this scheme suffers from user assaults and the opponent can readily forge a legal customer to access the network service and, also this scheme is unable to provide mutual authentication [10].

5.4 Mutual Key Authentication and Management: In network communications, key exchanging between two parties is very important. A secret symmetric key must be shared between two communicating parties with a help of trusted server. This is type of authenticated key exchanging is called three party key exchange. This key is used for mutual authentication and secure communication. This key authentication must be satisfied by the following requirements: Mutual authentication, Session key security, Perfect forward secrecy.

- **Improved Mutual Authentication Scheme:** This scheme offers effective safety, improved performance and greater effectiveness than the Wu system. WBANs using IoT technology provide a straightforward, low-cost health surveillance and telemedicine approach for elders. Presently most literature shows that for authentication schemes generally using SBP but this proposed scheme is using ABP as mentioned is section 5.2. This scheme has done security feature analysis for Mutual authentication & Key agreement, user anonymity & untraceability, perfect forward security, replay attack, message tamper attack and impersonation attack. Hence, it is proved that this model is providing reliable security and withstands various network threats. The performance analysis has done on client and application provider and compared the result with [18] and [22]. The final data on communication cost has demonstrated that the proposed [10] scheme is having higher cost than [22] and lower than [18].
- **Mutual Authenticated Key Agreement Scheme [5]:** The proposed secure scheme that addresses the problems, identified in [28], of different types of attacks like Offline Identity Guessing Attacks (OIGA), Sensor Imitation Attacks (IMA) and Hub Spoofing Attacks (HSA) and reclaims the efficiency in wireless sensors nodes and mobile phones. Li in [28] stated that this WBAN protocol permits unauthorized communication so that an opponent cannot connect any of the communication session to some another session of the same SN. But, the authors in [5] demonstrated that the claim is not true. The performance evaluation of this key agreement scheme fulfilled the following security properties: Security against anonymity, tracking attacks, insider attacks, replay attacks, impersonation attacks, mutual authentication and forward secrecy session key. The authors have ensures that the proposed architecture may be considered for designing any authentication.
- **Authenticated Key Exchange Protocol [7]:** Two authenticated key exchange protocols are suggested in [7] based on symmetric cryptosystem. This system supports selective authentication between WBAN nodes. [7]. this scheme is supporting the selective authentication between nodes in WBAN. The simulation result is shown that it unable to break the attacks such as trivial substitution and attack of replay, man in the middle attack and the attack of fake base station. The authors observed that the time consuming for cryptographic operations on either side of the communicating parties and on the third party. Therefore the experimental result shows that it requires less computational time and energy efficiency for the proposed works than the existing protocols. The two schemes are proved as secure models in BAN logic model. Normally, a timestamp is used to guarantee the freshness of messages. But the proposed models have adopted random number instead of timestamp which is reducing the network's complexity and reducing costs. Analysis of performance demonstrates that protocols have superior runtime performance, lower memory expenses.
- **Enhanced Secure Sensor Association and Key Management [8]:** In WBAN, there may be a group of sensors are deployed in order to observe different bio-signals. Since the data is to be communicated among the group of sensors, the security and privacy is important in the e-healthcare system. So, there is a need for safe sensor connection and the management of key system based on ECC. In WBAN networks, the data confidentiality, integrity is the required parameters for the security and association. The authors in [8] have developed a Secure Sensor Association (SSA) and Key Management Scheme (KMS) based on ECC. Also this is recommended for power and resource constrained sensor nodes in BANs.

  In this work hash chains are used to perform authentication and, a secret key that was shared between each Sensor Node (SN) and Patient Controller (PC) is calculated using ECC. Here, a group key is calculated by PC and assumed that Key Generation Center (KGC) is secure and trustworthy. Moreover the sensor nodes do not trust each other before association is made. The security analysis of this work has demonstrated to withstand that there no opponent can learn the shared secret and the group keys and also the opponent cannot impersonate the other party with other entities. Also, the mutual authentication is provided between the PC and HWD.

5.5 Remote Authentication

- **Remote Authentication Scheme [17]:** A secure communication scheme design must satisfy the properties such as privacy, truthfulness, ease of use, non-refutation and ambiguity. But this was a challengeable job for each proposed schemes. Cryptography methods are most commonly used or using for providing data and communication security. However, this method requires high computation time and thus most literature says that public key or symmetric key based cryptosystems are not efficient or suitable for WBAN. The authors in [17] have used the concepts as described in sections 5.1, 5.2 and 5.3. The proposed scheme is demonstrated for WBANs is secure under random oracle model and it is a certificate less authentication model. The system is used a super singular elliptic curve $y^2=x^3+1$ to attain the same level of security as 1024-bit in the algorithm of RSA. In order to calculate the communication cost, the algorithm is assuming the length of p=512 bits and q=160 bits respectively and the length of an element in G_1=1024 and G_2=512 respectively. The contact overhead during login and response for the proposed scheme is 1536 bits and 1216 bits respectively. The simulation result has shown that the proposed WBAN remote authentication protocol diminishes the client side running time by half.
- **Authentication scheme for Telecare Medical Information System (TMIS) [20]:** The authentication scheme in [20] is a new TMIS remote authentication scheme with authenticated public keys that is officially safe in the ID-mBJM model. To provide greater security and better scalability, dozens of anonymous authentication schemes for TMIS have been proposed. The authentication scheme [20] used TMIS bilinear pairings based on privacy authentication. This model is uses a hash function and is done a security analysis based on random oracles model. The proposed mathematical model and its concerned simulation results have demonstrated that the security of this model is robust against the possible attacks such as user privacy, forward secrecy, known key security and off-line password guessing attack and replay attack. The estimation cost in authentication and login phase of the proposed scheme is compared with [21], [23], [26], [27] and show that this scheme has better computational efficiency. Also the authors in [20] informed to the research groups that their work is provably secure in the oracle model.

5.6 Comparison Analysis of Authentication schemes for WBANs

As the WBAN customer and software provider communicates with each other through an open wireless medium. An adversary controls this medium of WBAN communication and also endures from different types of attacks. So, there is a necessity to consider over the progress of various requirements in security for the design of secure authentication model with free of errors. In our research [10, 11, 17-23, 26, 27], the certain most needed security requirements and the robustness of the security schemes against attacks are considered. and, the detailed analyses are shown in Table I .

Table I: Analysis of Resistance to various attacks

SR/ Ref.	10	11	17	19	20	27	28	29	31	32
IMP	S	S	S	S	-	-	S	S	NS	S
SVA	-	S	S	S	S	S	S	S	NS	NS
MOD	S	-	-	-	-	-	-	-	-	-
UNL	-	-	S	-	-	-	-	-	-	-
UNT	S	-	-	-	-	-	-	-	-	-
KKS	-	S	-	S	S	S	S	S	S	S
NKS	-	S	-	-	-	-	S	-	-	-
RPL	S	-	-	S	S	S	-	S	S	NS
MMA	-	-	-	S	-	-	-	S	S	NS
PDI	-	-	-	S	-	-	-	S	S	S
RMT	-	-	-	S	-	-	-	NS	NS	NS
MTA	S	-	-	-	-	-	-	-	-	-
NPT	-	-	S	-	S	NS	-	-	-	-
PGA	-	-	-	-	S	S	-	-	-	-
PPP	-	-	-	-	S	NS	-	-	-	-

SR: Security Requirements, **Ref**.: Reference Number
IMP: Impersonation, **SVA**: Stolen Verifier Attack Resilience, **MOD**: Modification, **UNL**: Unlinkability, **UNT**: Untraceability, **KKS**: Known Key Security, **NKS**: No Key Security, **RPL**: Replay Attack, **MMA**: Man-in-Middle Attack, **PDI**: Privacy and Data Integrity, **RTM**: Real Time Monitoring, **MTA**: Message Tamper Attack, **NPT**: No Password or Verifier Table, **PGA**: Prevention of off-line Password Guessing Attack, **PPP**: Preserving Patient Privacy, **PPS**: Provision of Provable Security
S: Satisfied, **NS**: Not Satisfied, **-**: No mention

A quantitative performance evaluation of computational cost includes modular exponentiation, elliptic curve scale multiplication, hashing and bilinear pairing operations. The running time of different operations on client and application provider is shown in Table II.

The estimation costs of both customer and application provider in the authentication phase among different schemes are evaluated in Table III.

Table II: Analysis of Running Time in Application Provider (AP) and Client (C) in ms

SR/ Ref.	[23] -v1	[23] -v2	[21]	[22]	[17]	[10]	[32]
AP	39.83	39.63	38.28	32.80	44.66	39.63	13.61
C	186.19	186.19	92.01	188.36	92.01	-	146.44

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table III: Comparison of computation cost in authentication phase

Protocols	Client	Application Providers
Chen et al.'s Scheme [5]	$3T_{SM}+T_{ME}$=155.52 ms	$5T_{SM}+T_{BP}$ = 51.94 ms
Li et al.'s Scheme [6]	$2T_{mul}+1T_h+1T_k$	$1T_h+1T_k+1T_b$
Liu et al.'s – Protocol I [7]	15.968 ms	9.655 ms
Liu et al.'s – Protocol II [7]	14.894 ms	10.729 ms
Omala et al.'s Scheme [13]	-	7 T_{SM}=44.66 ms
Guo et al.'s Scheme [20]	-	$4T_h+2T_s+T_p+3T_m$
Zhao's Scheme [21]	$3T_p+4T_h+1T_{mm}+1T_{mas}+T_{sys}$=92.01 ms	$6T_p+5T_h+T_{sys}$=38.29 ms
Liu et al.'s -I Scheme [23]	$1T_{ME}+4T_p+3T_h+1T_{mas}$ = 186.19 ms	$1T_{ME}+1T_{PM}+1T_p+3T_h+1T_{mm}+1T_{mi}$=39.83 ms
Liu et al.'s-II Scheme [23]	$1T_{ME}+4T_p+3T_h+1T_{mas}$ = 186.19 ms	$1T_{ME}+1T_{PM}+1T_p+3T_h+1T_{mm}+1T_{mi}$=39.83 ms
Xiong's Scheme [24]	$5T_{mul}+2T_{add}+5T_h$	$3T_{mul}+4T_{add}+3T_h$
Jiang et al.'s Scheme [25]	$3T_{mul}+4T_h+1T_k+1T_b$	$3T_{mul}+4T_h+1T_k+1T_b$
Islam et al.'s Scheme [26]	-	$4T_p+5T_m+2T_s+5T_h$
Li et al.'s Scheme [27]	-	$4T_p+5T_m+2T_s+5T_h$
Li et al.'s Scheme [28]	-	$9T_h$

5.7 Securing Medical data through Block chain Concepts

In the recent and upcoming ultramodern worlds' platform, mini and microelectronic devices are ruling and going to rule in all dimensions of human life. So, today's environment peoples are using android based mobile phones as the one of the main communication devices. In the healthcare sector, to keep the medical record as secret as possible Block Chain (BC) technologies are used. BC is an electronic ledger that registers digital currency transfers and other important patient information involving people's lives.

Remote Patient Monitoring using Block chain [14]: The authors have proposed by utilizing BC based smart contracts to provide safe study and supervision of sensors in medical field. This system has made use of permission, consortium-managed BC to execute smart contracts. The smart contracts are a method for the estimation of data collected from patient's using IoT health monitoring devices.

Nowadays, healthcare data are the well-paid target for hacker. So, there is a need to preserve the electronic health records and that should be manageable, transferable. To address this kind of issue the authors have projected a system with smart contracts on a consortium-managed BC. The authors have mentioned that the reason for using BC is that it has the ability to enhance security of patients using remote monitoring systems. In this work, the device oracle provides communications directly to dealers. For necessary alertness for the patients, a threshold values are fixed according to the individual contracts. The smart contracts are implemented and coded using the Ethereum coding language Solidity and Remix respectively. The security analysis has done by the authors with the following metrics and compared with traditional system: Confidentiality, Availability, Immutability, Traceability, Speed, Privacy and Transparency.

Also this paper has the following shortfalls: 1) On large scale of transactions the key management model is to be designed to manage too many numbers of keys. 2) With the present constraints of the proposed system, it may not work for emergency response. 3) Even though algorithms like PBFT is used, sometimes person-based verification is needed before any new node is inserted in to the system to avoid the existence of scoundrel miners. It would be better if we are allowing the healthcare to use the concept of big data with additional consistent information for getting better results.

VI. CONCLUSION

In this paper, securities with authentication protocols and key management protocols have been reviewed. Also, the pros and cons of each paper is discussed and analyzed. During the analysis, various security requirements and various attacks have been studied and tabulated in this article. The efficiencies of the algorithms are studied with running time and computation cost in authentication phase, and also tabulated with this paper. The study shows that the new techniques which are used in WBAN and its issues are discussed. Since WBAN is considering the improvement of the quality of human life, particularly for the elder persons, the medical data have to be placed or transferred with utmost security level. Nowadays, hardware and software technologies are utmost in high end. In future, the researchers have to find out the best data protection method. In order to achieve this high level trust worthy security for medical data, Block chain concepts are highly recommended.

REFERENCES

1. https://esa.un.org/unpd/wpp/Publications/Files/WPP2017_KeyFindings.pdf.
2. Shihong Zou, Yanhong Xu, Honggang Wang, Zhouzhou Li, Shanzhi Chen and Bo Hu, "A Survey on Secure Wireless Body Area Networks," Journal of Security and Communication Networks,2017, pp.1-9.
3. Samaher Al-Janabi, Ibrahim Al-Shourbaji, Mohammad Shojafar, Shahaboddin Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," Egyptian Informatics Journal, 2017, pp. 113-122.
4. Wencheng Sun, Zhiping Cai, Yangyang Li, Fang Liu, Shengqun Fang and Guoyan Wang, "Security and Privacy in the Medical Internet of Things: A Review," Journal of Security and Communication Networks, 2018, pp. 1-9.
5. Chien-Ming Chen, Bing Xiang, Tsu-Yang Wu and King-Hang Wang, "An Anonymous Mutual Authenticated Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks", Journal of Applied Sciences, July, 2018, pp. 1-15.
6. Tong Li, Yuhui Zheng, and Ti Zhou, "Efficient Anonymous Authenticated Key Agreement Scheme for Wireless Body Area Networks," Journal of Security and Communication Networks, 2017, pp. 1-8.
7. Jingwei Liu, Qian Li, Rui Yan and Rong Sun, "Efficient authenticated key exchange protocols for wireless body area networks," EURASIP Journal on Wireless Communications and Networking, 2015.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

8. Jian Shen, Haowen Tan, Sangman Moh, Ilyong Chung, Qi Liu, and Xingming Sun, "Enhanced Secure Sensor Association and Key Management in Wireless Body Area Networks," Journal of Communications and Networks, October, 2015, Vol. 17, No. 5.
9. Samaneh Movassaghi et al., "A Review of Routing Protocols in Wireless Body Area Networks", Journal of Networks, 2013, Vol. 8, No. 3.
10. Chen, R. & Peng, D., "Analysis and Improvement of a Mutual Authentication Scheme for Wireless Body Area Networks", J Med Syst ,2019,Vol. 43,No. 19.
11. Liu, X., Jin, C. & Li, F., "An Improved Two-Layer Authentication Scheme for Wireless Body Area Networks," J Med Syst, Vol. 42,2018, No. 143.
12. Sharavanan, P.T., Sridharan, D. & Kumar, R., "A Privacy Preservation Secure Cross Layer Protocol Design for IoT Based Wireless Body Area Networks Using ECDSA Framework", J Med Syst,vol. 42,No. 196,2018.
13. Omala, A.A., Mbandu, A.S., Mutiria, K.D. et al., "Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network," J Med Syst,vol. 42,no. 108, 2018.
14. Griggs, K.N., Ossipova, O., Kohlios, C.P. et al., "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring", J Med Syst, 2018, vol.42,no.130.
15. Firdaus, A., Anuar, N.B., Razak, M.F.A. et al., "Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management", J Med Syst, 2018, vol. 42, no. 112.
16. Murtaza Cicioglu, Ali Calhan, "IoT based wireless body area networks for disaster cases," Int. Journal of Communication System, December 2018.
17. Omala, A.A., Kibiwott, K.P. & Li, F., "An Efficient Remote Authentication Scheme for Wireless Body Area Network," J Med Syst, vol. 41, no. 25, 2017.
18. Wu, L., Zhang, Y., Li, L and Shen, J., "Efficient and Anonymous Authentication Scheme for Wireless Body Area Networks", J Med Syst, vol. 40, no. 134, 2016.
19. Li, CT., Lee, CC. & Weng, CY., "A Secure Cloud-Assisted Wireless Body Area Networks in Mobile Emergency Medical Care System", J Med Syst, vol. 40,no. 117,2016.
20. Guo, D., Wen, Q., Li, W. et al., "A Novel Authentication Scheme Using Self-certified Public Keys for Telecare Medical Information Systems," J Med Syst, vol.39, no. 62, 2015.
21. Zhao, Z., "An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem," J Med Syst, vol. 38, no. 13, 2014.
22. Wang, C., and Zhang, Y., "New authentication scheme for wireless body area networks using the bilinear pairing", J. Med. Syst., vol. 39, no. 11, pp. 1-8, 2015.
23. Liu, J., Zhang, Z., Chen, X., and Kwak, K. S., "Certificateless remote anonymous authentication schemes for wireless body sensor networks", IEEE Trans. Parallel Distrib. Syst. , vol. 25,no. 2,pp. 332-342, 2014.
24. H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," IEEE Transactions on Information Forensics and Security, Vol. 9, no. 12, pp. 2327-2339, 2014
25. Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, and Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth," Journal of Medical Sytems, vol. 40, no. 11, 2016.
26. Islam, S.K., and Biswas, G.P., "A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosytem," Journal of System Software,vol. 84,no.11,pp.1892- 1898, 2011.
27. Li, C.T., "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card," IET Information Security, vol. 7, no. 1,pp. 3-10, 2013.
28. Li, X.; Ibrahim, M.H.; Kumari, S.; Sangaiah, A.K.; Gupta, V.; Choo, K.K.R., "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," Journal of Computer Networks, vol. 129, pp. 429-443, 2018.
29. Shen, J.; Gui, Z.; Ji,S.; Shen, J.; Tan, H.; Tang, Y, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," Journal of Network Computer Applications, vol. 106, no. 117-123,2018.
30. Chien-Ming Chen, Bing Xiang, Tsu-Yang Wu and King-Hang Wang, "An Anonymous Mutual Authenticated Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks," Journal of Applied Sciences, vol. 8, no. 1074, 2018.
31. R. Lu, Z. Cao, "Simple three-party key exchange protocol," Journal of Computer Security, vol. 26, no. 1, pp.94-97, 2007.
32. EJ Yoon, KY Yoo, "Improving the novel three-party encrypted key exchange protocol," Comput. Stand. Interfaces. 30(5), 309-314, 2008. http://www.(URL)

AUTHORS PROFILE

S. Ananthakumaran, has received M.E (Computer Science and Engineering) degree from Anna University, Tamilnadu, India in 2006. He has completed his Ph.D., in Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India. He has more than 16 years of academic and 9 years of research experience. Presently he is working as Associate Professor, Dept. of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. He is a life member of Cryptology Research Society of India (CRSI). His research area includes Blockchain Technology, Wireless Sensor Networks, Secure and energy efficient routing Algorithms, and Cyber Security..

Mrs. R. Bhavani graduated in Electrical and Electronics Engineering from Thiagarajar College of Engineering, Madurai, Tamil Nadu, and India in 2000. In 2005, she received Master of Engineering (M.E) degree in Power Systems Engineering in the same college. Now, she is doing her ph.D in the area of power quality under Anna University, Chennai. She had 3 years of teaching experience in PSNA College of Engineering and Technology, Dindigul. From 2009 to 2015, she was an Assistant Professor in the department of Electrical Engineering at Mepco Schlenk Engineering, Sivakasi, Tamil Nadu, and India. Since 2016, she has been as an Assistant professor (Sr.Grade) in the same college. She has submitted her PhD in the field of Power Quality (PQ) under Anna University, Chennai, India. Her area of interest are machines ,control systems, microprocessor and microcontroller and power systems Her research activities are focused on measurement and analysis of PQ problems, Applications of Custom Power Devices for PQ Enhancement using Artificial Intelligence Techniques, Lab VIEW software. She has published two papers in SCI indexed journals; three papers in Scopus indexed journals and six papers in IEEE conference. She is a life time member in ISTE and IEI..

Dr. K.Mohaideen Pitchai, has completed his doctoral degree in Information Communication Engineering under Anna University, Chennai during April 2015. He has published more than 10 international journals. He has completed 4 funded projects sponsored by various governmental agencies. He has filled 2 patent. his research area includes Adhoc & Sensor Networks and Theoretical Computer Science.